WHOLESALE EFT WORKPROGRAM

CHAPTER 18WP

(FILE NAME ON DISK # 3 = IS–WP#13.WPD)

COMMENTS

The objective of this section is to determine the adequacy of controls over an EFT environment. Although these applications should be operating outside of the IS environment, they depend highly on computer operations. The procedures are set up so that they may be implemented separately as part of either the IS or safety and soundness bank examinations. The examiner should document any findings, especially those which do not satisfy the recommendations in *1996 FFIEC IS Examination Handbook*.

Tier I

GENERAL

1. Obtain or prepare a description of all wholesale EFT applications employed by the institution.

2. For each identified EFT application, obtain or prepare an organization chart.

3. Determine the adequacy of insurance coverage for each EFT operation and the overall EFT environment.

4. Review the minutes of management committees responsible for overall or any specific EFT activity for content and follow-up of any material matters set forth.

WHOLESALE OR LARGE DOLLAR FUNDS TRANSFER SYSTEMS (FTS)

5. Obtain or prepare a flowchart (or detailed narrative) of the overall FTS. Review the information to determine the degree of automated interface, linkage to functions not supported by the FTS and separation of duties/functions considering:

   a. Fedwire.
   b. CHIPS or other local payments system.
   c. SWIFT.
   d. Telex.
   e. Internal transfers (book entry).
   f. Customer networks.
   g Internal networks.

h. Other payment origination sources (e.g., telephone, fax, mail, internal memos, standing instructions).

i. Testing of payment origination messages.

6. Review policies and procedures in place to monitor customer balances for outgoing payments to ensure that payments are made against collected funds or established intraday or overnight overdraft limits and that payments resulting in excesses of established uncollected or overdraft limits are properly authorized.

7. Review the adequacy of security procedures in place for both outgoing and incoming payment orders for each step of the FTS process considering:

   a. Payment order origination (e.g., message testing for telex, telephone, letters/memos, fax).

   b. Data entry.

   c. Payment order execution/release.

   d. Telecommunications lines.

   e. Physical security.

8. Review a sample of contracts authorizing the institution to make payments from a customers account to ensure that they adequately set forth responsibilities of the institution and the customer, primarily regarding provisions of the Uniform Commercial Code Article 4A (UCC4A) related to authenticity and timing of transfer requests.

9. Review the disaster recovery plan for the FTS to ensure that it is reasonable in relation to the volume of activity and that all units of the FTS are provided for in the plan and regularly tested. Consider the CHIPS requirement for participants that originate more than $20 billion daily transfer value for Fedwire and CHIPS combined.

10. Review the audit program to ensure all functions of the FTS are covered, including:

a. Payment order origination (funds transfer requests).

b. Message testing.

c. Customer agreements.

d. Payment processing and accounting.

e. Personnel policies.

f. Physical and data security.

g. Contingency plans.

h. Credit evaluation and approval.

i. Incoming funds transfers.

j. Bank Secrecy and OFAC issues.

k. Federal Reserve's Payment Systems Risk Program.

11. Compare the last executed internal audit procedures covering each of the areas noted in step 10 above, to the related questions detailed in Tier II of these procedures, and determine whether they meet or exceed Tier II coverage.

12. Review a sufficient sample of supporting audit workpapers necessary to confirm that they support the execution of procedures established in step 11 above.

13. Review all audit reports related to the FTS and determine the current status of any exceptions noted in the audit report.

BSA and OFAC REVIEW

14. Determine if the wire transfer area maintains reports to identify potential money laundering activities (BSA).

15. Determine if the wire transfer area maintains OFAC identification and reporting capabilities.

16. If there are any shortfalls in identification or recordkeeping under steps 14 or 15 above refer to the EIC and/or your agencies Compliance/BSA subject matter expert(s) (SME).

17. Consistent with the scope of the examination, procedures included in Tier II that are not sufficiently covered under steps 11 and 12, above, are to be implemented as part of this examination . (Note: To the extent coverage is clearly satisfactory and current, audit procedures and workpapers also may be used to address steps 6 through 9).

CONCLUSIONS

18. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

19. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

20. Assign rating. (See the Chapter 5 for additional information.)

21. Prepare an index of workpapers for this section of the workprogram.

22. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable,

recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

23. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier I Addendum
FEDWIRE THIRD-PARTY ACCESS ARRANGEMENTS

The following procedures should be used, as appropriate

The Federal Reserve Board allows, under certa in conditions, a depository institution (the participant) to designate another depository institution or entity (the service provider) to in itiate, receive or otherwise process Fedwire funds transfers and book-entry securities transfers that are posted to its reserve or clearing account held at the Federal Reserve Bank. Such third-party access arrangements are permitted providing the specific conditions outlined in section G of the Federal Reserve Policy Statement on Payments System Risk (FRRS 9-1016) have been met. If Fedwire funds and/or book-entry securities transfer operations are performed by a service provider:

1. Ensure that the participant retains control o f the credit-granting process by individuall y approving each funds/securities transfer o r establishing individua l customer transfer limits and a transfer limit for the participant's ow n activity, within which the service provider can act.

2. Determine whether the service provider:

   a. Obtains the participant's permission to initiate transfers that would exceed individual customer credit limits or the transfer limit for the participant's own activity.

   b. Notifies the participant of incoming book-entry securities transfers that exceed the applicable limit, and determine that the participant's instructions to accept or reverse the transfer are processed by the service provider in a timely manner.

3. Determine whether:

   a. All Fedwire transfer activity is posted to the participant's account and that the institution maintains responsibility for its account.

   b. Participant has the ability to monitor transfer activity conducted on its behalf.

4. Determine if the participant's board of directors has approved the following:

   a. The role and responsibilities of a service provider (that is not affiliated with the participant through at least 80 percent common ownership).

   b. That in a L/C arrangement, the intraday overdraft limit for the activity to be processed by the service provider and the credit limits for any inter-affiliate funds transfers.

5. Assess whether the participant has adequate contingency backup capabilities for its transfer activities as set forth in the *Interagency Policy On Contingency Planning for Financial Institutions, FFIEC SP-5.*

6. For arrangements where the service provider is not affiliated with the participant through at least 80 percent common ownership, determine that the participant is able to continue Fedwire operations if the participant is unable to continue its service provider arrangement in the event the participant's primary supervisor terminated the arrangement.

7. Determine if the participant has certified that the arrangement is consistent with corporate separateness and does not violate branching restrictions.

8. Assess whether the participant has certified that the arrangement will allow the participant to comply with all applicable state and federal laws and regulations governing the participant, including retaining and making accessible records in accordance with the regulations adopted under the Bank Secrecy Act.

9. Determine if the participant's primary supervisor has affirmatively stated in writing that it does not object to the arrangement.

10. Determine whether:

    a. Ensure that the participant has in place an adequate audit program to review the third-party access arrangement at least annually.

    b. In the case of an arrangement involving a foreign service provider,

ensure that the participant and the service provider have in place an adequate audit program that addresses Fedwire operations and that reports are made available to the Federal Reserve and the participant's primary U. S. supervisor(s) in English. (This program should confirm compliance with the provisions stipulated in section G of the Federal Reserve Board's Payments System Risk Policy.)

11. Assess whether the service provider is subject to examination by the appropriate federal depository institution regulatory agency(s).

12. Determine if the participant and the service provider(s) have executed an agreement with the relevant Reserve Bank(s) incorporating the conditions stipulated in the Fedwire third-party access policy.

CONCLUSIONS

13. Proceed to procedure 18, Tier 1.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

Negative response/determinations should be discussed with , management , their remedy, compensating controls and the examiner's comments should be recorded in the workpapers.

WHOLESALE OR LARGE DOLLAR FUNDS TRANSFER SYSTEMS

Funds transfer requests

1. Does the funds transfer function maintain a current list of bank personnel authorized to initiate transfer requests?

2. Does the bank limit the number of employees who can initiate or authorize transfer requests?

3. Are authorized employee signature records kept in a secure environment?

4. Are standard, sequentially numbered, forms used by bank personnel to initiate funds transfer requests?

5. If standard forms are not used in certain circumstances (e.g., telephone requests from remote offices) is an authentication system used?

6. Does the bank employ an adequate security procedure for requests received from customers via telex, on-line terminals, telephone, fax, or written instructions?

7. Is more than signature verification (e.g., tests, call backs) required on written requests (e.g. memos, letters, fax)?

8. Does the bank maintain a current record of authorized signers for customers who use the bank's funds transfer services and does it include authorized sources (e.g., telephone, memo, fax)?

9. Does the bank advise its customers to limit the number of authorized signers?

10. Are customer signature records maintained under dual control or otherwise protected?

	Comments
11. Do customer authorization lists limit the amount that an individual is authorized to transfer?	
12. Has the bank established guidelines for what information should be obtained from a person making a funds transfer request?	
13. Do the records of transfer requests contain:	
a. The account title and number?	
b. A sequence number?	
c. The amount to be transferred?	
d. The person or other source initiating the request?	
e. The time and date?	
f. Authentication?	
g. Paying instructions?	
h. Bank personnel authorizing certain types and dollar amount transfers?	
14. Does the bank have procedures in effect to prohibit persons who receive transfer requests from transmitting or accounting for those requests?	
15. Does the bank use devices that record all incoming and outgoing telephone transfer requests?	
16. If calls are recorded, does the bank advise its customers in written contracts, by audible bleeping signals, or by informing the caller that telephone calls are being recorded?	
17. Does the funds transfer function maintain sequence control internally for requests that it processes?	

18. Are incoming and outgoing messages time stamped or sequentially numbered for control?

19. Are transfer requests recorded in a log or another bank record before execution?

20. Is the log or record of transfer requests reviewed daily by supervisory personnel?

21. If not sequentially accounted for, is an unbroken copy of all messages received via telex or other terminal printers kept throughout the business day?

22. Are sequence records and unbroken copies reviewed and controlled by someone not connected with equipment operations?

TEST KEYS

23. If test keys are used for authentication, are the files containing test key formulas maintained under dual control or otherwise protected?

24. Are only authorized personnel permitted in the test key area or allowed access to terminals used for test key purposes?

25. Does the bank maintain an up-to-date test key file?

26. Does management maintain a list of those persons who have access to test key files?

27. Are all messages and transfer requests that require testing authenticated by the use of a test key?

28. Are test codes verified by someone other than the person receiving the initial transfer request?

29. Does the bank's test key formula incorporate a variable (e.g., sequence number) and is the requirement stated in an agreement between the bank and the customer?

30. Does the bank have procedures in operation for the issuance and cancellation of test keys?

31. Is the responsibility for issuing and canceling test keys assigned to someone who is not responsible for testing the authenticity of transfer requests?

AGREEMENTS

32. Are agreements in effect concerning funds transfer operations between the financial institution and its customers, correspondent banks, systems providers (e.g., Federal Reserve Bank and CHIPS), servicers, and hardware/software vendors?

33. Do the agreements fix responsibilities and accountability between all parties?

34. Do agreements with customers adequately describe the security procedures as defined by UCC Article 4A Sections 201 and 202?

35. Does the bank obtain written waivers from its customers if they chose security procedures that are different from what is offered by the bank, as indicated in UCC Article 4A Section 202(c)?

36. Do agreements with customers establish cut-off times for receipt and processing of payment orders and canceling or amending payment orders as noted in UCC Article 4A Section 106?

PAYMENT PROCESSING AND ACCOUNTING

37. Does the funds transfer department of the bank prepare a daily reconcilement of funds transfer activity (incoming and outgoing) by dollar amount and number of messages?

38. Does the funds transfer department perform end-of-day reconcilements for messages sent to and received from intermediaries (e.g., Federal Reserve Bank, servicers, correspondents, and clearing facilities)?

39. Are all pre-numbered forms, including cancellations, accounted for in the daily reconcilement?

40. Are reconcilements of funds transfer and message requests reviewed daily by supervisory personnel?

41. Is the balancing of the daily activity separate from the receiving, processing, and sending functions?

42. Does the funds transfer department verify that work sent to and received from other bank departments agrees with its totals?

43. Is someone responsible for reviewing all transfer requests to determine that they have been properly processed?

44. Are key fields reverified before transmission and are messages released by someone other than the individual originally entering the message?

45. Are all rejects and/or exceptions reviewed by someone not involved in the receipt, preparation, or transmittal of funds?

46. If the institution accepts transfer requests after the close of business or transfer requests with a future value date, are they properly controlled and processed?

47. Are Federal Reserve Bank, correspondent bank and clearing house statements used for funds transfer activities reconciled and reviewed daily in another area of the bank (e.g., accounting or correspondent banking) to determine that they agree with the funds transfer departments records and the reasons for any *open* funds transfer items?

48. Are open statement items, suspense accounts, receivables/payables, and inter-office accounts related to funds transfer activity controlled outside of the funds transfer operations?

49. Are periodic reports on open statement items, suspense accounts and inter-office accounts prepared for management and do the reports include aging of open items, the status of significant items and resolution of prior significant items?

50. Are corrections, overrides, open items, reversals, and other adjustments reviewed and approved by an officer?

51. Are all general ledger tickets, or other supporting documents initialed by the originator and supervisory personnel?

	Comments
52. Does the bank maintain adequate records as required by the Currency and Foreign Transactions Reporting Act of 1970 (also known as the Bank Secrecy Act)?	
PERSONNEL	
53. Has the bank taken steps to ensure that screening procedures are applied to personnel hired for sensitive positions in the funds transfer department?	
54. Does the bank prohibit new employees from working in sensitive areas of the funds transfer operation unless they are closely supervised?	
55. Are temporary employees excluded from working in sensitive areas? If not, is the number of such employees limited and are they closely supervised?	
56. Are statements of indebtedness required of employees in sensitive positions of the funds transfer function?	
57. Are employees subject to unannounced rotation of responsibilities?	
58. Are relatives of employees in the funds transfer function precluded from working in the same institution's bookkeeping, audit and data processing functions, and/or in departments generating funds transfer requests?	
59. Does the bank's policy require that employees take a minimum number of consecutive days as part of their annual vacation and is the policy being enforced?	
60. Does management reassign employees who have given notice of resignation or have been given termination notices, from sensitive areas of the funds transfer function?	
PHYSICAL AND DATA SECURITY	
61. Is access to the funds transfer area restricted to authorized personnel?	

	Comments
62. Are visitors to the funds transfer area identified, required to sign in, and be accompanied at all times?	
63. Is written authorization by department management given to those employees who remain in the funds transfer area after normal working hours and are security guards informed?	
64. Are bank terminal operators or others in funds transfer operations denied access to computer equipment areas or programs?	
65. Do procedures prohibit computer personnel from gaining access to bank terminals or test key information used for funds transfers?	
66. Does funds transfer equipment have physical and/or software locks to prohibit access by unauthorized personnel at all times?	
67. Are terminals and other hardware in the funds transfer area shut down after normal working hours and or regulated by automatic time-out controls or time-of-day controls?	
68. Are passwords suppressed on terminals when being entered?	
69. Are operator passwords changed and, if so, are they changed at reasonable intervals?	
70. Is supervisory approval required for terminal access made at other than authorized times?	
71. Are passwords restricted to different levels of activity (e.g., input, release, and adjustments) and to data files?	
72. Is terminal operator training conducted in a manner that will not jeopardize the integrity of live data or memo files?	
73. Are employees prohibited from taking keys for sensitive equipment out of the funds transfer area?	
74. Does the bank maintain back-up systems for events such as equipment failures and line malfunctions?	

75. Are back-up systems periodically tested by bank personnel?

76. Does the use of back-up equipment require approval by supervisory personnel?

77. Are procedures and controls in place to prevent the inadvertent release of test data into the production environment, thus transferring live funds over the system?

CONTINGENCY PLANS

78. Have written contingency plans been developed for partial or complete failure of the systems and/or communication lines between the bank and correspondent bank, servicer, CHIPS, Federal Reserve Bank, and data centers. Do the procedures, at a minimum, ensure recovery by the opening of the next day's processing?

79. Are these contingency plans reviewed regularly and tested periodically?

80. Has management distributed these plans to all funds transfer personnel?

81. Are sensitive information and equipment adequately secured before evacuation in an emergency and is further access to the affected areas denied by security personnel?

CREDIT EVALUATION AND APPROVAL

82. Does the funds transfer department or another area of the bank have procedures in effect to prohibit transfers of funds against accounts that do not have collected balances or preauthorized credit availability?

83. Have customer limits been established for intraday and overnight overdrafts?

    a. Are groups of affiliated customers included in such limits?

    b. Are funds transfers activities monitored during the business day to ensure that payments

causing limits to be exceeded are not executed without proper approval?

c. Are the limits reviewed and updated?

d. Are the customer limits revised by senior management at reasonable intervals?

84. Does the bank make payments in anticipation of the receipt of covering funds? If so, are such payments approved by officers with appropriate credit authority?

85. Are intraday exposures limited to amounts expected to be received the same day?

86. Are intraday overdraft limits established giving consideration to other types of credit facilities for the same customer?

87. Is an intraday record kept for each customer showing opening collected and uncollected balances, transfers in and out, and the collected balances at the time payments are released?

88. If payments exceed the established limits, are they referred to a person(s) with appropriate credit authority before releasing payments and steps taken in a timely manner to obtain covering funds?

89. When an overnight overdraft limit is exceeded, is a determination made as to whether a fail caused the overdraft? If so, is this properly documented? Is adequate follow-up made to obtain the covering funds in a timely manner?

90. Where required as a participant of a net settlement system (e.g., CHIPS), are bi-lateral credit limits set based on a formal credit analysis and are the limits approved by the appropriate level of management?

91. If the institution is an Edge Act corporation do intraday and overnight overdrafts comply with Regulation K?

INCOMING FUNDS TRANSFERS

92. Are incoming payments not received over a secure system (e.g., Fedwire), such as book entry

transfer requests received via telex or phone, authenticated prior to processing?

93. Are separation of duties maintained over receipt of instructions, posting to a customers account, and mailing of customer credit advices?

94. Are audit trails maintained from receipt through posting to a customers account?

95. Is issuance of customer advices timely?

96. Are incoming credits accurately accounted for throughout the process?

PAYMENT SYSTEM RISK

97. If the institution incurs overdrafts in its Federal Reserve Account, has the Payment System Risk program been completed (i.e., has the institution selected an appropriate net debit cap)?

98. If the institution has elected a de minimis or self-assessment net debit cap, ensure that the examination evaluates the adequacy of records supporting the institution's program and accuracy of the de minimis or self-assessment rating.

POLICY AND STANDARDS

99. Do standards exist for:

    a. Software and hardware *acquisition* including:

        1) Cost benefit analysis?
        2) Programming standards?
        3) Documentation Standards?
        4) Ownership of programs, spreadsheets, etc. developed on the institution's time and equipment?
        5) Escrow of source code of critical, tailor-made funds transfer software to ensure the institution can continue to maintain software in event of failure of vendor?

    b. Micro/mini computer use including:

        1) Use of the output/data?
        2) Restrictions on personal and nonjob related use?

3) Use of personal equipment and/or software?
4) Use of unauthorized software?
5) Modification of the hardware and or software?
6) Copying or piracy of the software?
7) File backup?

100. Have housekeeping procedures been developed and enforced to provide protection from:

a. Food?

b. Liquids?

c. Dust, smoke?

d. Magnetic fields?

101. Have procedures been developed and enforced for:

a. Backup and off-site storage of critical information?

b. Inventory control on the hardware software?

102. Have adequate security measures been established covering:

a. Physical security.

1) Restricted area.
2) Key locks on the machines.
3) Removing and securing the data files.

b. Access controls.

1) Passwords.
2) Encryption of data on the disk.
3) Use of dial-up equipment.
4) Read only attributes to the files.

103. Proceed to procedure 18, Tier I.

Examiner | Date

_____|_____

Reviewer's Initials